Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Into
ER 85-4994

Office of Legislative Liaison

Routing Slip

TO:	ACTION	INFO
1. D/OLL		
2. DD/OLL		X
3. Admin Officer		X
4. Liaison		
5. Legislation		
		X
		X
		X
9.		
10.		
SUSPENSE		

Date

Action Officer:

Remarks:

GJ / 20 Dec 85
Name/Date

STAT

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

EXECUTIVE SECRETARIAT
ROUTING SLIP

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	EXDIR		X		
4	D/ICS				
5	DDI		X		
6	DDA		X		
7	DDO		X		
8	DDS&T		X		
9	Chm/NIC				
10	GC		X		
11	IG		X		
12	Compt	X			
13	D/OLL		X		
14	D/PAO		X		
15	D/PERS				
16	VC/NIC				
17					
18					
19					
20					
21					
22					
	SUSPENSE				

Date

Remarks To 12: for action as appropriate. (Merry Christmas!! Interesting memo from OMB in that, as mention is made of paperwork reduction, we get this easy to read/follow 26 page document! But I guess there are paper savings, since it is printed on 2 sides!)

STAT

Executive Secretary
19 Dec 85
Date

3637 (10-81)

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Recpt # Record

Executive Registry
85- 4994

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

December 12, 1985

CIRCULAR NO. A-130

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Management of Federal Information Resources

1. Purpose: This Circular establishes policy for the management of Federal information resources. Procedural and analytic guidelines for implementing specific aspects of these policies are included as appendices.

2. Rescissions: This Circular rescinds OMB Circulars No. A-71, A-90, A-108, and A-121, and all Transmittal Memoranda to those circulars.

3. Authorities: This Circular is issued pursuant to the Paperwork Reduction Act of 1980 (44 U.S.C. 35); the Privacy Act of 1974 (5 U.S.C. 552a), Sections 111 and 206 of the Federal Property and Administrative Services Act of 1949 as amended (40 U.S.C. 759 and 487, respectively), the Budget and Accounting Act of 1921 as amended (31 U.S.C. 11), Executive Order No. 12046 of March 27, 1978, and Executive Order No. 12472 of April 3, 1984.

4. Applicability and Scope:

a. The policies in this Circular apply to the information activities of all agencies of the executive branch of the Federal Government.

b. Information classified for national security purposes should also be handled in accordance with the appropriate national security directives. National security emergency preparedness activities should be conducted in accordance with Executive Order No. 12472.

5. Background: The Paperwork Reduction Act establishes a broad mandate for agencies to perform their information management activities in an efficient, effective, and economical manner. To assist agencies in an integrated approach to information resources management, the Act requires that the Director of the Office of Management and Budget (OMB) develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

6. Definitions: As used in this Circular--

a. The term "agency" means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only the Office of Management and Budget and the Office of Administration.

b. The term "information" means any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape.

c. The term "government information" means information created, collected, processed, transmitted, disseminated, used, stored, or disposed of by the Federal Government.

d. The term "information system" means the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

e. The term "major information system" means an information system that requires special continuing management attention because of its importance to an agency mission; its high development, operating or maintenance costs; or its significant impact on the administration of agency programs, finances, property, or other resources.

f. The term "access to information" refers to the function of providing to members of the public, upon their request, the government information to which they are entitled under law.

g. The term "dissemination of information" refers to the function of distributing government information to the public, whether through printed documents, or electronic or other media. "Dissemination of information" does not include intra-agency use of information, interagency sharing of information, or responding to requests for "access to information."

h. The term "information technology" means the hardware and software used in connection with government information, regardless of the technology involved, whether computers, telecommunications, micrographics, or others. For the purposes of this Circular, automatic data processing and telecommunications activities related to certain critical national security missions, as defined in 44 U.S.C. 3502 (2) and 10 U.S.C. 2315, are excluded.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

i. The term "information technology facility" means an organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology.

j. The term "information resources management" means the planning, budgeting, organizing, directing, training, and control associated with government information. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and technology.

k. The term "government publication" means informational matter which is published as an individual document at government expense, or as required by law.

Other definitions specific to the subjects of the appendices appear in the appendices.

7. Basic Considerations and Assumptions

a. The Federal Government is the largest single producer, consumer, and disseminator of information in the United States. Because of the size of the government's information activities, the dependence of government information activities upon the public's cooperation, and the value of government information to the entire Nation, the management of Federal information resources is an issue of continuing importance to the public and to the government itself.

b. Government information is a valuable national resource. It provides citizens with knowledge of their government, society, and economy--past, present, and future; is a means to ensure the accountability of government; is vital to the healthy performance of the economy; is an essential tool for managing the government's operations; and is itself a commodity often with economic value in the marketplace.

c. The free flow of information from the government to its citizens and vice versa is essential to a democratic society. It is also essential that the government minimize the Federal paperwork burden on the public, minimize the cost of its information activities, and maximize the usefulness of government information.

d. In order to minimize the cost and maximize the usefulness of government information activities, the expected public and private benefits derived from government information, insofar as they are calculable, should exceed the public and private costs of the information.

e. Although certain functions are inherently governmental in nature, being so intimately related to the public interest as to mandate performance by Federal employees, the government

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

should look first to private sources, where available, to provide the commercial goods and services needed by the government to act on the public's behalf, particularly when cost comparisons indicate that private performance will be the most economical.

f. The use of up-to-date information technology offers opportunities to improve the management of government programs, and access to, and dissemination of, government information.

g. Because the public disclosure of government information is essential to the operation of a democracy, the public's right of access to government information must be protected in the management of Federal information resources.

h. The individual's right to privacy must be protected in Federal Government information activities involving personal information.

i. The open and efficient exchange of government scientific and technical information, subject to applicable national security controls and proprietary rights others may have in such information, fosters excellence in scientific research and the effective use of Federal research and development funds.

j. The value of preserving government records is a function of the degree to which preservation protects the legal and financial rights of the government or its citizens, and provides an official record of Federal agency activities for agency management, public accountability, and historical purposes.

k. Federal Government information resources management policies and activities can affect, and be affected by, the information policies and activities of other nations.

8. Policies

a. Information Management. Agencies shall:

(1) Create or collect only that information necessary for the proper performance of agency functions and that has practical utility, and only after planning for its processing, transmission, dissemination, use, storage, and disposition;

(2) Seek to satisfy new information needs through legally authorized interagency or intergovernmental sharing of information, or through commercial sources, where appropriate, before creating or collecting new information;

(3) Limit the collection of individually identifiable information and proprietary information to that which is legally authorized and necessary for the proper performance of agency functions;

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(4) Maintain and protect individually identifiable information and proprietary information in a manner that precludes:

(a) Unwarranted intrusion upon personal privacy (see Appendix I); and

(b) Violation of confidentiality;

(5) Provide individuals with access to, and the ability to amend errors in, systems of records, consistent with the Privacy Act;

(6) Provide public access to government information, consistent with the Freedom of Information Act;

(7) Ensure that agency personnel are trained to safeguard information resources;

(8) Disseminate information, as required by law, describing agency organization, activities, programs, meetings, systems of records, and other information holdings, and how the public may gain access to agency information resources;

(9) Disseminate such information products and services as are:

(a) Specifically required by law; or

(b) Necessary for the proper performance of agency functions, provided that the latter do not duplicate similar products or services that are or would otherwise be provided by other government or private sector organizations;

(10) Disseminate significant new, or terminate significant existing, information products and services only after providing adequate notice to the public;

(11) Disseminate such government information products and services:

(a) In a manner that ensures that members of the public whom the agency has an obligation to reach have a reasonable ability to acquire the information;

(b) In the manner most cost effective for the government, including placing maximum feasible reliance on the private sector for the dissemination of the products or services in accordance with OMB Circular No. A-76; and

(c) So as to recover costs of disseminating the products or services through user charges, where appropriate, in accordance with OMB Circular No. A-25;

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(12) Establish procedures for:

(a) Reviewing periodically the continued need for and manner of dissemination of the agency's information products or services; and

(b) Ensuring that government publications are made available to depository libraries as required by law.

b. Information Systems and Information Technology Management. Agencies shall:

(1) Establish multiyear strategic planning processes for acquiring and operating information technology that meet program and mission needs, reflect budget constraints, and form the bases for their budget requests;

(2) Establish systems of management control that document the requirements that each major information system is intended to serve; and provide for periodic review of those requirements over the life of the system in order to determine whether the requirements continue to exist and the system continues to meet the purposes for which it was developed;

(3) Make the official whose program an information system supports responsible and accountable for the products of that system;

(4) Meet information processing needs through interagency sharing and from commercial sources, when it is cost effective, before acquiring new information processing capacity;

(5) Share available information processing capacity with other agencies to the extent practicable and legally permissible;

(6) Acquire information technology in a competitive manner that minimizes total life cycle costs;

(7) Ensure that existing and planned major information systems do not unnecessarily duplicate information systems available from other agencies or from the private sector;

(8) Acquire off-the-shelf software from commercial sources, unless the cost effectiveness of developing custom software is clear and has been documented;

(9) Acquire or develop information systems in a manner that facilitates necessary compatibility;

(10) Assure that information systems operate effectively and accurately;

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(11) Establish a level of security for all agency information systems commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information systems (See Appendix III);

(12) Assure that only authorized personnel have access to information systems;

(13) Plan to provide information systems with reasonable continuity of support should their normal operations be disrupted in an emergency;

(14) Use Federal Information Processing and Telecommunications Standards except where it can be demonstrated that the costs of using a standard exceed the benefits or the standard will impede the agency in accomplishing its mission;

(15) Not require program managers to use specific information technology facilities or services unless it is clear and is convincingly documented, subject to periodic review, that such use is the most cost effective method for meeting program requirements;

(16) Account for the full costs of operating information technology facilities and recover such costs from government users as provided in Appendix II;

(17) Not prescribe Federal information system requirements that unduly restrict the prerogatives of heads of State and local government units;

(18) Seek opportunities to improve the operation of government programs or to realize savings for the government and the public through the application of up-to-date information technology to government information activities.

9. Assignment of Responsibilities:

a. All Federal Agencies. The head of each agency shall:

(1) Have primary responsibility for managing agency information resources;

(2) Ensure that the information policies, principles, standards, guidelines, rules, and regulations prescribed by OMB are implemented appropriately within the agency;

(3) Develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular;

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(4) Develop agency policies and procedures that provide for timely acquisition of required information technology;

(5) Maintain an inventory of the agencies' major information systems and information dissemination programs;

(6) Create, maintain, and dispose of a record of agency activities in accordance with the Federal Records Act of 1950, as amended;

(7) Identify to the Director, OMB, statutory, regulatory, and other impediments to efficient management of Federal information resources and recommend to the Director legislation, policies, procedures, and other guidance to improve such management;

(8) Assist OMB in the performance of its functions under the Paperwork Reduction Act, including making services, personnel, and facilities available to OMB for this purpose to the extent practicable;

(9) Appoint a senior official, as required by 44 U.S.C. 3506(b), who shall report directly to the agency head, to carry out the responsibilities of the agency under the Paperwork Reduction Act. The head of the agency shall keep the Director, OMB, advised as to the name, title, authority, responsibilities, and organizational resources of the senior official. For purposes of this paragraph military departments and the Office of the Secretary of Defense may each appoint one official.

b. Department of State. The Secretary of State shall:

(1) Advise the Director, OMB, on the development of United States positions and policies on international information policy issues affecting Federal Government information activities and ensure that such positions and policies are consistent with Federal information resources management policy;

(2) Ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international information technology standards, and advise the Director, OMB, of such activities.

c. Department of Commerce. The Secretary of Commerce shall:

(1) Develop and issue Federal Information Processing Standards and guidelines necessary to ensure the efficient and effective acquisition, management, security, and use of information technology;

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(2) Advise the Director, OMB, on the development of policies relating to the procurement and management of Federal telecommunications resources;

(3) Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of information technology;

(4) Conduct studies and evaluations concerning telecommunications technology, and concerning the improvement, expansion, testing, operation, and use of Federal telecommunications systems and advise the Director, OMB, and appropriate agencies of the recommendations that result from such studies;

(5) Develop, in consultation with the Secretary of State and the Director, OMB, plans, policies, and programs relating to international telecommunications issues affecting government information activities;

(6) Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;

(7) Ensure that the Federal Government is represented in the development of national and, in consultation with the Secretary of State, international information technology standards, and advise the Director, OMB, of such activities.

d. Department of Defense. The Secretary of Defense shall develop, in consultation with the Administrator of General Services, uniform Federal telecommunications standards and guidelines to ensure national security, emergency preparedness, and continuity of government.

e. General Services Administration. The Administrator of General Services shall:

(1) Advise the Director, OMB, and agency heads on matters affecting the procurement of information technology;

(2) Coordinate and, when required, provide for the purchase, lease, and maintenance of information technology required by Federal agencies;

(3) Develop criteria for timely procurement of information technology and delegate procurement authority to agencies that comply with the criteria;

(4) Provide guidelines and regulations for Federal agencies, as authorized by law, on the acquisition, maintenance, and disposition of information technology;

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(5) Develop policies and guidelines that facilitate the sharing of information technology among agencies as required by this Circular;

(6) Review agencies' information resources management activities to meet the objectives of the triennial reviews required by the Paperwork Reduction Act and report the results to the Director, OMB;

(7) Manage the Automatic Data Processing Fund and the Federal Telecommunications Fund in accordance with the Federal Property and Administrative Services Act, as amended;

(8) Establish procedures for approval, implementation, and dissemination of Federal telecommunications standards and guidelines and for implementation of Federal Information Processing Standards.

f. Office of Personnel Management. The Director, Office of Personnel Management, shall:

(1) Develop and conduct training programs for Federal personnel on information resources management, including end user computing;

(2) Evaluate periodically future personnel management and staffing requirements for Federal information resources management;

(3) Establish personnel security policies and develop training programs for Federal personnel associated with the design, operation, or maintenance of information systems.

g. National Archives and Records Administration. The Archivist of the United States shall:

(1) Administer the Federal records management program in accordance with the National Archives and Records Act;

(2) Assist the Director, OMB, in developing standards and guidelines relating to the records management program.

h. Office of Management and Budget. The Director of the Office of Management and Budget shall:

(1) Provide overall leadership and coordination of Federal information resources management within the executive branch;

(2) Serve as the President's principal adviser on procurement and management of Federal telecommunications systems, and develop and establish policies for procurement and management of such systems;

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(3) Issue policies, procedures, and guidelines to assist agencies in achieving integrated, effective, and efficient information resources management;

(4) Initiate and review proposals for changes in legislation, regulations, and agency procedures to improve Federal information resources management;

(5) Review and approve or disapprove agency proposals for collection of information from the public, as defined in 5 CFR 1320.7;

(6) Develop and publish annually, in consultation with the Administrator of General Services, a five-year plan for meeting the information technology needs of the Federal government;

(7) Evaluate agencies' information resources management and identify cross-cutting information policy issues through the review of agency information programs, information collection budgets, information technology acquisition plans, fiscal budgets, and by other means;

(8) Provide policy oversight for the Federal records management function conducted by the National Archives and Records Administration and coordinate records management policies and programs with other information activities;

(9) Review, with the advice and assistance of the Administrator of General Services, selected agencies' information resources management activities to meet the objectives of the triennial reviews required by the Paperwork Reduction Act;

(10) Review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance with the Privacy Act and related statutes;

(11) Resolve information technology procurement disputes between agencies and the General Services Administration pursuant to Section 111 of the Federal Property and Administrative Services Act;

(12) Review proposed U.S. government position and policy statements on international issues affecting Federal Government information activities and advise the Secretary of State as to their consistency with Federal information resources management policy.

10. Oversight. The Director, OMB, will use information technology planning reviews, fiscal budget reviews, information collection budget reviews, management reviews, GSA reviews of agency information resources management activities, and such

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

other measures as he deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this Circular.

11. Effective Date. This Circular is effective upon publication.

12. Inquiries. All questions or inquiries should be addressed to Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-3287.

13. Sunset Review Date. This Circular shall have an independent policy review to ascertain its effectiveness three years from the date of issuance.

James C[illegible]er III
Director

Appendix I: Federal Agency Responsibilities for Maintaining Records about Individuals

Appendix II: Cost Accounting, Cost Recovery, and Interagency Sharing of Information Technology Facilities

Appendix III: Security of Federal Automated Information Systems

Appendix IV: Analysis of Key Sections

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

APPENDIX I
TO OMB CIRCULAR NO. A-130

FEDERAL AGENCY RESPONSIBILITIES FOR MAINTAINING RECORDS ABOUT INDIVIDUALS

1. Purpose and Scope

This Appendix describes agency responsibilities for implementing the Privacy Act of 1974, 5 U.S.C. 552a as amended (hereinafter "the Act"). It applies to all agencies subject to the Act. The Appendix constitutes a revision to procedures formerly contained in OMB Circular No. A-108, now rescinded. Note that this Appendix does not rescind other guidance OMB has issued to help agencies interpret the Privacy Act's provisions, e.g., Privacy Act Guidelines (40 Federal Register 28949-28978, July 9, 1975), or Guidance for Conducting Matching Programs (47 Federal Register 21656-21658, May 19, 1982).

2. Definitions

a. The terms "agency," "individual," "maintain," "record," "system of records," and "routine use," as used in this Appendix, are defined in the Act (5 U.S.C. 552a (a)). The definition of "agency" in the Act differs somewhat from the definition in the Circular.

b. The term "minor change to a system of records" means a change that does not significantly change the system; that is, does not affect the character or purpose of the system and does not affect the ability of an individual to gain access to his or her record or to any information pertaining to him or her which is contained in the system; e.g., changing the title of the system manager.

3. Assignment of Responsibilities

a. All Federal Agencies. In addition to meeting the agency requirements contained in the Act, and the specific reporting requirements detailed in this Appendix, the head of each agency shall ensure that the following reviews are conducted as often as specified below, and be prepared to report to the Director, OMB, the results of such reviews and the corrective action taken to resolve problems uncovered. The head of each agency shall:

(1) Section (m) Contracts. Review every two years a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

accomplish an agency function, in order to ensure that the wording of each contract makes the provisions of the Act apply. (5 U.S.C. 552a (m)(1))

(2) Recordkeeping Practices. Review annually agency recordkeeping and disposal policies and practices in order to assure compliance with the Act.

(3) Routine Use Disclosures. Review every three years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency originally collected the information. The first such review should commence immediately upon the issuance of this Appendix.

(4) Exemption of Systems of Records. Review every three years each system of records for which the agency has promulgated exemption rules pursuant to Section (j) or (k) of the Privacy Act in order to determine whether such exemption is still needed.

(5) Matching Programs. Review annually each ongoing matching program in which the agency has participated during the year, either as a source or as a matching agency, in order to ensure that the requirements of the Act, the OMB Matching Guidelines, and the OMB Model Control System and Checklist have been met.

(6) Privacy Act Training. Review annually agency training practices in order to ensure that all agency personnel are familiar with the requirements of the Act, with the agency's implementing regulation, and with any special requirements that their specific jobs entail.

(7) Violations. Review annually the actions of agency personnel that have resulted either in the agency being found civilly liable under Section (g) of the Act, or an employee being found criminally liable under the provisions of Section (i) of the Act, in order to determine the extent of the problem and to find the most effective way to prevent recurrences of the problem.

(8) Systems of Records Notices. Review annually each system of records notice to ensure that it accurately describes the system. Where minor changes are needed, ensure that an amended notice is published in the Federal Register. Agencies may choose to make one annual comprehensive publication consolidating such minor changes. This requirement is distinguished from and in addition to the requirement to report to OMB and the Congress major changes to systems of records and to publish those changes in the Federal Register (see paragraph 4b of this Appendix).

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

b. Department of Commerce. The Secretary of Commerce shall, consistent with guidelines issued by the Director, OMB, develop and issue standards and guidelines for assuring the security of information protected by the Privacy Act in automated information systems.

c. General Services Administration. The Administrator of General Services shall, consistent with guidelines issued by the Director, OMB, issue instructions on what agencies must do in order to comply with the requirements of Section (m) of the Act when contracting for the operation of a system of records to accomplish an agency purpose.

d. Office of Personnel Management. The Director of the Office of Personnel Management shall, consistent with guidelines issued by the Director, OMB:

(1) Develop and maintain government-wide standards and procedures for civilian personnel information processing and recordkeeping directives to assure conformance with the Act.

(2) Develop and conduct training programs for agency personnel, including both the conduct of courses in various substantive areas (e.g., legal, administrative, information technology) and the development of materials that agencies can use in their own courses. The assignment of this responsibility to OPM does not affect the responsibility of individual agency heads for developing and conducting training programs tailored to the specific needs of their own personnel.

e. National Archives and Records Administration. The Archivist of the United States shall, consistent with guidelines issued by the Director, OMB:

(1) Issue instructions on the format of the agency notices and rules required to be published under the Act.

(2) Compile and publish annually the rules promulgated under 5 U.S.C. 552a(f) and agency notices published under 5 U.S.C. 552a (e)(4) in a form available to the public.

(3) Issue procedures governing the transfer of records to Federal Records Centers for storage, processing, and servicing pursuant to 44 U.S.C. 3103. For purposes of the Act, such records are considered to be maintained by the agency that deposited them. The Archivist may disclose deposited records only according to the access rules established by the agency that deposited them.

f. Office of Management and Budget. The Director of the Office of Management and Budget will:

(1) Issue guidelines and directives to the agencies to implement the Act.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(2) Assist the agencies, at their request, in implementing their Privacy Act programs.

(3) Review the new and altered system reports agencies submit pursuant to Section (o) of the Act.

(4) Compile the annual report of the President to the Congress in accordance with Section (p) of the Act.

4. Reporting Requirements

a. Privacy Act Annual Reports. To provide the necessary information for the annual report of the President, agencies shall submit a Privacy Act Annual Report to the Director, OMB, covering their Privacy Act activities for the calendar year. The exact format and timing of the report will be established by the Director, OMB. (5 U.S.C. 552a (p)); but, agencies should, at a minimum collect, and be prepared to report the following data on a calendar year basis:

(1) Total number of active systems of records and changes to that population during the year, e.g., publications of new systems, additions and deletions of routine uses, exemptions, automation of record systems.

(2) Public comments received on agency publications and implementation activities.

(3) Number of requests from individuals for access to records about themselves in systems of records that cited the Privacy Act in support of their requests.

(4) Number granted in whole or part, denied in whole, and for which no record was found.

(5) Number of amendment requests from individuals to amend records about them in systems of records that cited the Privacy Act in support of their requests.

(6) Number granted in whole or part, denied in whole, and for which no record was found.

(7) Number of appeals of access and amendment denials and the results of such appeals.

(8) Number of instances in which individuals litigated the results of appeals of access or amendment, and the results of such litigation.

(9) Number and description of matching programs participated in either as source or matching agency.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

b. New and Altered System Reports. The Act requires agencies to publish notices in the Federal Register describing new or altered systems of records, and to submit reports on these systems to the Director, OMB, and to the Congress.

(1) Altered System of Records. Minor changes to systems of records need not be reported. For example, a change in the designation of the system manager due to a reorganization would not require a report, so long as an individual's ability to gain access to his or her records is not affected. Other examples include changing applicable safeguards as a result of a risk analysis, deleting a routine use when there is no longer a need for the authorized disclosure. These examples are not intended to be all-inclusive.

The following changes are those for which a report is required:

(a) An increase or change in the number or types of individuals on whom records are maintained. For example, a decision to expand a system that originally covered only residents of public housing in major cities to cover such residents nationwide would require a report. Increases attributable to normal growth should not be reported.

(b) A change that expands the types or categories of information maintained. For example, a personnel file that has been expanded to include medical records would require a report.

(c) A change that alters the purpose for which the information is used.

(d) A change to equipment configuration (either hardware or software) that creates substantially greater access to the records in the system. For example, locating interactive terminals at regional offices for accessing a system formerly accessible only at the headquarters would require a report.

(e) The addition of an exemption (pursuant to Sections (j) or (k) of the Act). Note that, in submitting a rulemaking for an exemption as part of a report of a new or altered system, agencies will meet the reporting requirements of Executive Order No. 12291 and need not make a separate submission under that order.

When an agency makes a change to an information technology installation, telecommunication network, or any other general changes in information collection, processing, dissemination, or storage that affect multiple systems of records, it may submit a single consolidated new or altered system report, with changes to existing notices and supporting documentation included in the submission.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(2) Contents of the Report. The report for a new or altered system has three elements: a transmittal letter, a narrative statement, and supporting documentation that includes a copy of the proposed Federal Register notice. There is no prescribed format for either the letter or the narrative statement. The notice must appear in the format prescribed by the Office of the Federal Register's Document Drafting Handbook.

(a) Transmittal Letter. The transmittal letter should be signed by the senior agency official responsible for implementation of the Act within the agency and should contain the name and telephone number of the individual who can best answer questions about the system. The letter should contain the agency's assurance that the proposed system does not duplicate any existing agency systems. It should also state that a copy of the report has been distributed to the Speaker of the House and the President of the Senate as the Act requires. The letter may also include requests for waiver of the reporting time period.

(b) Narrative Statement. The narrative statement should be brief. It should make reference, as appropriate, to information in the supporting documentation rather than restating such information. The statement should:

1 Describe the purpose for which the agency is establishing the system of records.

2 Identify the authority under which the system is maintained. The agency should avoid citing housekeeping statutes, but rather cite the underlying programmatic authority for collecting, maintaining, and using the information. When the system is being operated to support an agency housekeeping program, e.g., a carpool locator, the agency may, however, cite a general housekeeping statute that authorizes the agency head to keep such records as are necessary.

3 Provide the agency's evaluation of the probable or potential effects of the proposal on the privacy of individuals.

4 Describe the relationship of the proposal, if any, to the other branches of the Federal Government and to State and local governments.

5 Provide a brief description of the steps taken by the agency to minimize the risk of unauthorized access to the system of records. A more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established shall be made available to OMB upon request.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

6 Explain how each proposed routine use satisfies the compatibility requirement of subsection (a)(7) of the Act. For altered systems, this requirement pertains only to any newly proposed routine uses.

7 Provide OMB control numbers, expiration dates, and titles of any OMB approved information collection requirements contained in the system of records. If the request for OMB clearance of an information collection is pending, the agency may simply state the title of the collection and the date it was submitted for OMB clearance.

(c) Supporting Documentation. Attach the following to all new or altered system reports:

1 An advance copy of the new or altered system notice (consistent with the provisions of 5 U.S.C. 552a (e)(4)) that the agency proposes to publish for the new or altered system. For proposed altered systems the documentation should be in the same form as the agency proposes to publish in the public notice.

2 An advance copy of any new rules or changes to published rules (consistent with the provision of 5 U.S.C. 552a (f), (j), and (k)) that the agency proposes to issue for the new or altered system. If no changes to existing rules are required, the agency shall so state in the narrative portion of the report. Proposed changes to existing rules shall be provided in the same form as the agency proposes to publish for formal notice and comment.

(3) Timing and Distribution for Submitting New and Altered System Reports. Submit reports on new and altered systems of records not later than 60 days prior to establishment of a new system or the implementation of an altered system (5 U.S.C. 552a (o)). Submit three copies of each report to:

President of the Senate
Washington, D.C. 20510

Speaker of the House of Representatives
Washington, D.C. 20515

Administrator
Office of Information and Regulatory Affairs
Office of Management and Budget
Washington, D.C. 20503

Agencies may assume that OMB concurs in Privacy Act aspects of their proposal if OMB has not commented within 60 days from the date the transmittal letter was signed. Agencies may publish system and routine use notices as well as exemption rules in the Federal Register at the same time that they send the new or

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

altered system report to OMB and the Congress. The 60 day period for OMB and Congressional review and the 30 day notice and comment period for routine uses and exemptions will then run concurrently.

(4) Waivers of Report Time Period. The Director, OMB, may grant a waiver of the 60 day period if the agency asks for the waiver and can demonstrate compelling reasons. Agencies may assume that OMB concurs in their request if OMB has not commented within 30 days of the date the transmittal letter was signed. When a waiver is granted, the agency is not thereby relieved of any other responsibility or liability under the Act. Note that OMB cannot waive time periods specifically established by the Act. Agencies will still have to meet the statutory notice and comment periods required for establishing a routine use or claiming an exemption.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

facility for support of the facility and/or for general use by users of the facility. All software acquired or maintained by users of the facility is excluded.

(4) The physical facilities, including computer rooms; tape and disk libraries; stockrooms and warehouse space; office space; physical fixtures.

b. The term "full costs" means all significant expenses incurred in the operation of an information technology facility. The following elements are included:

(1) Personnel, including salaries, overtime, and fringe benefits of civilian and military personnel; training; and travel.

(2) Equipment, including depreciation for owned, capitalized equipment; equipment rental or lease; and direct expenses for noncapitalized equipment.

(3) Software, including depreciation for capitalized costs of developing, converting, or acquiring software; rental of for software; and direct expenses for noncapitalized acquisition of software.

(4) Supplies, including office supplies; data processing materials; and miscellaneous expenses.

(5) Contracted services, including technical and consulting services; equipment maintenance; data entry support; operations support; facilities management; maintenance of software; and telecommunications network services.

(6) Space occupancy, including rental and lease of buildings, general office furniture, and equipment; building maintenance; heating, air conditioning and other utilities; telephone services; power conditioning and distribution equipment and alternate power sources; and building security and custodial services.

(7) Intra-agency services, including normal agency support services that are paid by the installation.

(8) Interagency services, including services provided by other agencies and departments that are paid by the installation.

c. The term "user" means an organizational or programmatic entity that receives service from an information technology facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report either to the manager or director of the facility or to the same immediate supervisor.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

APPENDIX II
TO OMB CIRCULAR NO. A-130

COST ACCOUNTING, COST RECOVERY, AND INTERAGENCY SHARING OF INFORMATION TECHNOLOGY FACILITIES

1. Purpose

This Appendix establishes procedures for cost accounting, cost recovery, and interagency sharing of Federal information technology facilities. The Appendix revises procedures formerly contained in OMB Circular No. A-121, now rescinded.

2. Applicability

This Appendix applies to all information technology facilities that are operated by or on behalf of a Federal agency; provide information technology service to more than one user; operate one or more general management computers; and have obligations in excess of $3 million per year.

3. Definitions

a. The term "information technology facility" means an organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. An information technology facility includes:

(1) The personnel who operate computers or telecommunications systems; develop or maintain software; provide user liaison and training; schedule computers, prepare and control input data; control, reproduce, and distribute output data; maintain tape and disk libraries; provide security, maintenance, and custodial services; and directly manage or provide direct administrative support to personnel engaged in these activities.

(2) The owned or leased computer and telecommunications hardware, including central processing units; associated peripheral equipment such as disk drives, tape drives, drum storage, printers, card readers, and consoles; data entry equipment; data reproduction, decollation, booking, and binding equipment; telecommunications equipment including control units, terminals, modems, and dedicated telephone and satellite links provided by the facility to enable data transfer and access to users. Hardware acquired and maintained by users of the facility is excluded.

(3) The software, including operating system software, utilities, sorts, language processors, access methods, data base processors, and other similar multi-user software required by the

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

d. The term "general management computer" means a digital computer that is used for any purpose other than as a part of a process control system, space system, mobile system, or a system meeting one of the exclusions identified in the Department of Defense Authorization Act of 1982.

4. Accounting and Reimbursement for Sharing of Information Technology Facilities

a. Interagency Sharing. Agencies shall:

(1) Share their information technology facilities with users from other agencies to the maximum extent feasible;

(2) Document sharing arrangements, where the total annual reimbursement exceeds $500,000, with individual written agreements that identify:

(a) Services available for sharing;

(b) Service priority procedures and terms (e.g., quality performance standards) to be provided to each user;

(c) Prices to be charged for providing services;

(d) Reimbursement arrangements for services provided; and

(e) Arrangements for terminating the sharing agreement;

(3) Provide standard terms and conditions to users obtaining similar services insofar as possible;

(4) Include such sharing arrangements, when fully documented and part of a formal sharing program, in justifications to OMB for resource requests (see OMB Circular No. A-11, revised) and allocations. Direct funding by a shared facility should be requested only where exceptional circumstances preclude the user agency from using alternative sources.

b. Cost Accounting. Agencies shall account for the full cost of the operation of information technology facilities.

c. User Cost Distribution System. Agencies shall implement a system to distribute the full cost of providing services to all users. That system will:

(1) Be consistent with guidance provided in the Federal Information Processing Standards Publication No. 96, "Guidelines for Developing and Implementing a Charging System for Data Processing Services" (National Bureau of Standards, Department of Commerce, 1982).

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(2) Price each service provided by the facility to the users of that service on an equitable basis commensurate with the amount of resources required to provide that service and the priority of service provided. The price of individual transactions may be estimated provided that they are periodically reconciled to assure that the full costs of operations are equitably distributed among all users.

(3) Directly distribute to the recipient of the services the full costs of dedicated services, including applications developed and maintained; software unique to a single application; and telecommunications equipment, including control units, terminals, modems, and dedicated telephone or satellite links provided by the facility to enable data transfer and computer access to users.

d. Cost Recovery. Consistent with statutory authority, agencies shall:

(1) Submit periodic statements to all users of agency information technology facilities specifying the costs of services provided;

(2) Recover full costs from Federal users of the facility; and

(3) Recover costs from nonfederal users of the facilities consistent with OMB Circular No. A-25.

e. Accounting for Reimbursements Received. Agencies shall:

(1) Include resource requests for the amount of planned information technology use in user budget and appropriation requests;

(2) Assure that shared facilities reduce budget and appropriation requests by the amount of planned reimbursements from users;

(3) Prepare, at the close of each fiscal year, a report that documents in the agency's official records the full past year cost of operating information technology facilities that recover more than $500,000 per year from sharing reimbursements; and

(4) Use the portion of reimbursements arising from equipment and software depreciation for the replacement of equipment and software capital assets, provided such usage is included in the agency's budget.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

5. Selection of Information Technology Facilities to Support New Applications.

In selecting information technology facilities to support new applications, agencies shall establish a management control procedure for determining which facility will be used to support each significant application. This procedure shall ensure that:

(a) All alternative facilities are considered, including other Federal agency and nonfederal facilities and services;

(b) Agency rules do not require that priority be given to the use of in-house facilities; and

(c) The user of the application has primary responsibility for selecting the facility.

6. Assignment of Responsibilities

a. All Federal Agencies. The head of each agency shall:

(1) Establish policies and procedures and assign responsibilities to implement the requirements of this Appendix; and

(2) Ensure that contracts awarded for the operation of information technology facilities include provisions for compliance with the requirements of this Appendix.

b. General Services Administration. The Administrator of General Services shall:

(1) Ensure that information technology facilities designated as Federal Data Processing Centers comply with the procedures established by this Appendix;

(2) Ensure that provisions consistent with this Appendix are included in contracts for the operation of information technology facilities when acquiring services on behalf of an agency;

7. Implementation Requirements

Agencies shall implement the provisions of this Appendix effective at the beginning of fiscal year 1987.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

APPENDIX III
TO OMB CIRCULAR NO. A-130

SECURITY OF FEDERAL AUTOMATED INFORMATION SYSTEMS

1. Purpose

This Appendix establishes a minimum set of controls to be included in Federal automated information systems security programs; assigns responsibilities for the security of agency automated information systems; and clarifies the relationship between such agency security programs and internal control systems established in accordance with OMB Circular No. A-123, Internal Control Systems. The Appendix revises procedures formerly contained in Transmittal Memorandum No. 1 to OMB Circular No. A-71, now rescinded, and incorporates responsibilities from applicable national security directives.

2. Definitions

a. The term "automated information system" means an information system (defined in Section 6d of the Circular) that is automated.

b. The term "information technology installation" means one or more computer or office automation systems including related telecommunications, peripheral and storage units, central processing units, and operating and support system software. Information technology installations may range from information technology facilities such as large centralized computer centers to individual stand-alone microprocessors such as personal computers.

c. The term "sensitive data" means data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

d. The term "sensitive application" means an application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

e. The term "security specifications" means a detailed description of the safeguards required to protect a sensitive application.

3. Automated Information Systems Security Programs

Agencies shall assure an adequate level of security for all agency automated information systems, whether maintained in-house or commercially. Specifically, agencies shall:

- Assure that automated information systems operate effectively and accurately;

- Assure that there are appropriate technical, personnel, administrative, environmental, and telecommunications safeguards in automated information systems; and

- Assure the continuity of operation of automated information systems that support critical agency functions.

Agencies shall implement and maintain an automated information systems security program, including the preparation of policies, standards, and procedures. This program will be consistent with government-wide policies, procedures, and standards issued by the Office of Management and Budget, the Department of Commerce, the Department of Defense, the General Services Administration, and the Office of Personnel Management. Agency programs shall incorporate additional requirements for securing national security information in accordance with appropriate national security directives. Agency programs shall, at a minimum, include four primary elements: applications security, personnel security, information technology installation security, and security awareness and training.

a. Applications Security

(1) Management Control Process and Sensitivity Evaluation. Agencies shall establish a management control process to assure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications, and into significant modifications to existing applications. Management officials who are the primary users of applications should evaluate the sensitivity of new or existing applications being substantially modified. For those applications considered sensitive, the management control process shall, at a minimum, include security specifications and design reviews and systems tests.

(a) Security Specifications. Agencies shall define and approve security requirements and specifications prior to acquiring or starting formal development of the applications. The results of risk analyses performed at the information technology installation where the applications will be processed should be taken into account when defining and approving security

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

specifications for the applications. Other vulnerabilities of the applications, such as in telecommunications links, shall also be considered in defining security requirements. The views and recommendations of the information technology user organization, the information technology installation, and the individual responsible for security at the installation shall be considered prior to the approval of security specifications for the applications.

(b) Design Reviews and System Tests. Agencies shall conduct and approve design reviews and system tests, prior to placing the application into operation, to assure the proposed design meets the approved security specifications. The objective of the system tests should be to verify that required administrative, technical, and physical safeguards are operationally adequate. The results of the design reviews and system tests shall be fully documented and maintained in the official agency records.

(c) Certification. Upon completion of the system tests, an agency official shall certify that the system meets all applicable Federal policies, regulations, and standards, and that the results of the tests demonstrate that the installed security safeguards are adequate for the application.

(2) Periodic Review and Recertification. Agencies shall conduct periodic audits or reviews of sensitive applications and recertify the adequacy of security safeguards. Audits or reviews shall evaluate the adequacy of implemented safeguards, assure they are functioning properly, identify vulnerabilities that could heighten threats to sensitive data or valuable resources, and assist with the implementation of new safeguards where required. They are intended to provide a basis for recertification of the security of the application. Recertification shall be fully documented and maintained in the official agency records. Audits or reviews and recertifications shall be performed at least every three years. They should be considered as part of agency vulnerability assessments and internal control reviews conducted in accordance with OMB Circular No. A-123. Security or other control weaknesses identified shall be included in the annual internal control assurance letter and report required by Circular No. A-123.

(3) Contingency Plans. Agencies shall establish policies and assign responsibilities to assure that appropriate contingency plans are developed and maintained by end users of information technology applications. The intent of such plans is to assure that users can continue to perform essential functions in the event their information technology support is interrupted. Such plans should be consistent with disaster recovery and continuity of operations plans maintained by the installation at which the application is processed.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

b. Personnel Security. Agencies shall establish and manage personnel security policies and procedures to assure an adequate level of security for Federal automated information systems. Such policies and procedures shall include requirements for screening all individuals participating in the design, development, operation, or maintenance of sensitive applications as well as those having access to sensitive data. The level of screening required by these policies should vary from minimal checks to full background investigations, depending upon the sensitivity of the information to be handled and the risk and magnitude of loss or harm that could be caused by the individual. These policies shall be established for both Federal and contractor personnel. Personnel security policies for Federal employees shall be consistent with policies issued by the Office of Personnel Management.

c. Information Technology Installation Security. Agencies shall assure that an appropriate level of security is maintained at all information technology installations operated by or on behalf of the Federal Government (e.g., government-owned, contractor-operated installations).

(1) Assigning Responsibility. Agencies shall assign responsibility for the security of each installation to a management official knowledgeable in information technology and security matters.

(2) Periodic Risk Analysis. Agencies shall establish and maintain a program for the conduct of periodic risk analyses at each installation to ensure that appropriate, cost effective safeguards are incorporated into existing and new installations. The objective of a risk analysis is to provide a measure of the relative vulnerabilities and threats to an installation so that security resources can be effectively distributed to minimize potential loss. Risk analyses may vary from an informal review of a microcomputer installation to a formal, fully quantified risk analysis of a large scale computer system. The results of these analyses should be documented and taken into consideration by management officials when certifying sensitive applications processed at the installation. Such analyses should also be consulted during the evaluation of general controls over the management of information technology installations conducted in accordance with OMB Circular No. A-123. A risk analysis shall be performed:

(a) Prior to the approval of design specifications for new installations;

(b) Whenever a significant change occurs to the installations (e.g., adding a local area network; changing from batch to online processing; adding dial-up capability). Agency criteria for defining significant change shall be commensurate with the sensitivity of the data processed by the installation.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(c) At periodic intervals established by the agency commensurate with the sensitivity of the data processed, but not to exceed every five years if no risk analysis has been performed during that period.

(3) Disaster and Continuity Plan. Agencies shall maintain disaster recovery and continuity of operations plans for all information technology installations. The objective of these plans should be to provide reasonable continuity of data processing support should events occur that prevent normal operations at the installation. For large installations and installations that support essential agency functions, the plans should be fully documented and operationally tested periodically, at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption of information technology support.

(4) Acquisition Specifications. Agencies shall assure that appropriate technical, administrative, physical, and personnel security requirements are included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services, whether procured by the agency or by GSA. These security requirements shall be reviewed and approved by the management official responsible for security at the installation making the acquisition.

d. Security Awareness and Training Programs. Agencies shall establish a security awareness and training program to assure that agency and contractor personnel involved in the management, operation, programming, maintenance, or use of information technology are aware of their security responsibilities and know how to fulfill them. Users of information technology systems should be apprised of the vulnerabilities of such systems and trained in techniques to enhance security.

4. Assignment of Responsibilities

a. Department of Commerce. The Secretary of Commerce shall:

(1) Develop and issue standards and guidelines for assuring the security of Federal automated information systems;

(2) Establish standards, approved in accordance with applicable national security directives, for systems used to process sensitive information the loss of which could adversely affect the national security interest; and

(3) Provide technical assistance to Federal agencies in implementing Department of Commerce standards and guidelines.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

b. Department of Defense. The Secretary of Defense shall:

(1) Act, in accordance with applicable national security directives, as executive agent of the government for the security of telecommunications and automated information systems that process information the loss of which could adversely affect the national security interest; and

(2) Provide technical material and assistance to Federal agencies concerning security of Federal telecommunications and automated information systems.

c. General Services Administration. The Administrator of General Services shall:

(1) Issue policies and regulations for the physical and environmental security of computer rooms in Federal buildings consistent with standards issued by the Department of Commerce and the Department of Defense.

(2) Assure that agency procurement requests for computers, software, telecommunications services, and related services include security requirements. Delegations of procurement authority to agencies by GSA under mandatory programs, dollar threshold delegations, certification programs, or other so-called blanket delegations shall include requirements for agency specification of security requirements.

(3) Assure that information technology equipment, software, computer room construction, guard or custodial services, telecommunications services, and any other related services procured by GSA meet the security requirements established and specified by the user agency and are consistent with other applicable policies and standards issued by OMB, the Department of Commerce, the Department of Defense, and the Office of Personnel Management.

(4) Issue appropriate standards for the security of Federal telecommunications systems. Standards related to systems used to communicate sensitive information, the loss of which could adversely affect the national security interest, shall be developed and issued in accordance with applicable national security directives.

d. Office of Personnel Management. The Director, Office of Personnel Management, shall maintain personnel security policies for Federal personnel associated with the design, programming, operation, maintenance, or use of Federal automated information systems. Requirements for personnel checks imposed by these policies should vary commensurate with the risk and magnitude of loss or harm that could be caused by the individual. The checks may range from merely normal reemployment screening procedures to full background investigations.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

5. Reports

In their annual internal control report to the President and the Congress, required under OMB Circular No. A-123, agencies shall:

a. Describe any security or other control weaknesses identified during audits or reviews of sensitive applications or when conducting risk analyses of installations; and

b. Provide assurance that there is adequate security of agency automated information systems.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

APPENDIX IV
TO OMB CIRCULAR NO. A-130

ANALYSIS OF KEY SECTIONS

1. Purpose

The purpose of this Appendix is to provide a general context and explanation for the contents of the key sections of the Circular.

2. Background

The Paperwork Reduction Act of 1980, P.L. 96-511, 94 Stat 2812, codified at Chapter 35 of Title 44 of the United States Code, establishes a broad mandate for agencies to perform their information activities in an efficient, effective, and economical manner. Section 3504 of the Act provides authority to the Director, Office of Management and Budget (OMB), to develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

The Circular implements OMB authority under the Act with respect to Section 3504(b), general information policy, Section 3504(e), records management, Section 3504(f), privacy, and Section 3504(g), Federal automatic data processing and telecommunications; the Privacy Act of 1974 (5 U.S.C. 552a); Sections 111 and 206 of the Federal Property and Administrative Services Act of 1949, as amended (40 U.S.C. 759 and 487, respectively); the Budget and Accounting Act of 1921 (31 U.S.C. 1 et seq.); and Executive Order No. 12046 of March 27, 1978 and Executive Order No. 12472 of April 3, 1984, Assignment of National Security and Emergency Telecommunications Functions. The Circular complements 5 CFR 1320, Controlling Paperwork Burden on the Public, which implements other sections of the Paperwork Reduction Act dealing with controlling the reporting and recordkeeping burden placed on the public.

In addition, the Circular revises and consolidates policy and procedures in five existing OMB directives and rescinds those directives, as follows:

A-71 - Responsibilities for the Administration and Management of Automatic Data Processing Activities

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Transmittal Memorandum No. 1 to Circular No. A-71 - Security of Federal Automated Information Systems

A-90 - Cooperating with State and Local Governments to Coordinate and Improve Information Systems

A-108 - Responsibilities for the Maintenance of Records about Individuals by Federal Agencies

A-121 - Cost Accounting, Cost Recovery, and Interagency Sharing of Data Processing Facilities

OMB's review of the five existing policy directives led to the conclusion that much, but not all, of their content was procedural in nature, concerned chiefly with how policies were to be carried out. OMB determined that it was important clearly to distinguish the statement of policies from the procedures for implementing those policies. For this reason, the main body of the Circular consists of basic considerations and assumptions, policies, and assignments of responsibility; the appendices to the Circular consist of procedures for implementing various policies and with analysis of key sections.

OMB developed the main body of the Circular relying upon comments on the Federal Register notice as well as other forms of Federal agency and public input, principally meetings with interested parties. For the procedural revisions, OMB relied on the assistance of interagency task groups.

The revised contents of OMB Circular No. A-71, dealing with assignments of responsibilities, are in the main body of this Circular. The contents of OMB Circular No. A-90 are rescinded entirely, with the exception of a policy statement at Section 8 (b)(17) of this Circular. Revisions of the procedural aspects of the other three policy directives--Transmittal Memorandum No. 1 to A-71, A-108, and A-121--are appendices to this Circular. Appendices I, II, and III have the same prescriptive force as the Circular; Appendix IV is an explanatory document.

On September 17, 1984, the President signed National Security Decision Directive (NSDD) No. 145, National Policy on Telecommunications and Automated Information Systems Security. The NSDD requires that the Director, OMB, review for consistency with the NSDD, and amend as appropriate, OMB Circular No. A-71, Transmittal Memorandum No. 1. The Circular and Appendix III satisfy the NSDD requirement.

3. Analysis

Section 6. Definitions

f. Access to information. g. Dissemination of information. The Circular defines "access to information" as the function of providing to members of the public, upon their

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

request, the government information to which they are entitled under law. Access refers to those situations in which the government agency's role is passive; access is what the government's responsibilities are when the public comes to the government and asks for information the government has and the public is entitled to. "Dissemination," in the Circular's usage, refers to the function of distributing government information; dissemination connotes an active outreach by a government agency. Dissemination refers to those situations in which the government provides the public with information without the public having to come and ask for it.

The distinction between access and dissemination is posed in order to elaborate the responsibilities of Federal agencies for providing information to the public. Two fundamentally different situations exist: one in which the public goes to the agency to ask for information the agency holds and may or may not have disseminated; and one in which the agency chooses to take the information it holds to the public. In the first instance--access--Congress has provided specific statutory policy in the Freedom of Information Act (FOIA) and in the Privacy Act. These laws and policies concerning access to government information are explicit, well known, and now so widely accepted in practice by Federal agencies as not to require policy elaboration in this Circular. Agencies should know that, if members of the public ask for information subject to FOIA or the Privacy Act, the agencies should normally provide the information forthwith, because the public has a formal legal process for forcing the agencies to yield the information.

The relationship between access to and dissemination of information is explained below, in the discussion of 8a(8) through (12).

Section 7. Basic Considerations and Assumptions

Basic considerations and assumptions are statements that provide the underpinnings for the prescriptive policies in Section 8; they are not themselves policy statements. They are either derived from statutes or legislative history, or represent executive branch management philosophy as embodied in the Circular.

- Statements 7-a through 7-d provide the general context for management of Federal information resources.

- Statement 7-e summarizes policy found in OMB Circular No. A-76, Performance of Commercial Activities.

- Statement 7-f states a general predisposition to use up-to-date information technology to manage Federal information resources.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

- Statements 7-g and 7-h pertain to the Privacy Act and the Freedom of Information Act, respectively.

- Statement 7-i pertains to the National Science and Technology Policy, Organization and Priorities Act.

- Statement 7-j pertains to the Federal Records Act.

- Statement 7-k states a relationship between Federal information policy and international information policy.

Section 8. Policies.

This section is divided into two subsections that generally correspond to the twofold definition of information resources management in Section 6-b, namely, information itself and the resources associated with information.

a. Information Management. The Paperwork Reduction Act acknowledges that information is a valuable resource and should be managed as such. Proceeding from this premise, this subsection states policies concerning the management of Federal information.

(1) and (2). Information Collection and Sharing. The Circular's basic considerations and assumptions (Section 7) establish the value of government information activities. Without question, some information created or collected by Federal agencies is so vital that the American form of government, the economy, national security, and citizens' safety and wellbeing could not continue to exist in its absence. Nothing in this Circular is intended to diminish or derogate the creation or collection of such information, nor to serve as a pretext under which a Federal agency could damage the Nation's critical needs by failing to create or collect such information.

At the same time, the Paperwork Reduction Act was designed to remedy deficiencies Congress perceived in Federal information activities. In the words of the report of the House Committee on Government Operations (Report No. 96-835, p. 3):

> The legislation is the result of a growing concern that the way the Government collects, uses, and disseminates information must be improved. Inefficiencies in current Federal information practices drastically reduce the effectiveness of the Government while, at the same time, drowning our citizens in a sea of forms, questionnaires, and reports.

The Act intends that the creation or collection of information be carried out within the context of efficient, effective, and economical management. When Federal agencies create or collect

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

information--just as when they perform any other vital functions --they consume scarce resources and such activities must be continually scrutinized in light of good management principles. The applicable principles provided in the purposes of the Act are:

- to minimize the Federal paperwork burden for individuals, small businesses, State and local governments, and other persons;

- to minimize the cost to the Federal Government of collecting, maintaining, using, and disseminating information; and

- to maximize the usefulness of information collected by the Federal Government. (44 U.S.C. 3501)

Agencies must justify the creation or collection of information in the light of their statutory functions. Policy statement 8a(9) uses the standard, "necessary for the proper performance of agency functions," taken directly from the Paperwork Reduction Act (44 U.S.C. 3504 (c)(2)). Further, the policy statement includes the requirement that the information have practical utility, as defined in the Paperwork Reduction Act (44 U.S.C. 3502 (15)) and elaborated in Controlling Paperwork Burdens on the Public (5 CFR 1320). Note that practical utility includes characteristics pertaining to the quality of information such as accuracy, adequacy, and reliability, and that, in the case of general purpose statistics or recordkeeping, practical utility means that actual uses can be demonstrated (5 CFR 1320.7 (q)).

Good management and the requirement of practical utility dictate that agencies must plan from the outset for the steps in the information life cycle. The Act also stipulates that agencies must "formulate plans for tabulating the information in a manner which will enhance its usefulness to other agencies and to the public" (44 U.S.C. 3507 (a)(1)(C)). When creating or collecting information, agencies must plan how they will process and transmit the information, how they will use it, what provisions they will make for access to it, whether and how they will disseminate it, how they will store it, and finally, how the information will ultimately be disposed of. While agencies cannot at the outset achieve absolute certitude in planning for each of these processes, the requirement for information resources planning is clearly contained in the Act (44 U.S.C. 3506 (c)(1)), and the absence of adequate planning is sufficient reason not to create or collect information in the first place.

Before creating or collecting new information, agencies should look first to other agencies and the private sector so as not to duplicate existing information sources or services that would satisfy their needs. The Act requires that agencies shall not conduct or sponsor information collections unless they have eliminated collections "which seek to obtain information

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

available from another source within the Federal Government" ((44 U.S.C. 3507 (a)(1)(A)). Each agency must also "ensure its information systems do not overlap each other or duplicate the systems of other agencies" (44 U.S.C. 3506 (c)(2)). The Act also contains provisions governing the sharing of information between agencies (44 U.S.C. 3510). Applying the policy of OMB Circular No. A-76, the Circular also requires agencies to examine the possibility of acquiring the necessary information from private sector sources.

This is not to say that information creation or collection functions should be indiscriminately turned over to other agencies or to the private sector, but rather to say that agencies have an obligation to examine other potential sources of information which may satisfy agency needs. Some information can only be created or collected by Federal agencies themselves in the exercise of the government's sovereign powers. For some information, the government can satisfy its legitimate needs only when a Federal agency is the creation or collection agent. But other information needs can be met, and in many cases are routinely met, through existing services and sources in other agencies or the private sector. In many cases there is no inherently governmental function that is served by having information collected by a Federal agency; agencies should and do consider acquiring information collection services from the private sector. The Circular emphasizes that these sources should always be looked to first in the interests of efficiency and economy.

(3) through (6). Privacy Act and Freedom of Information Act. These statements contain policy statements pertaining to the Privacy Act and incorporating the policies of OMB Circular No. A-108, which is rescinded and superseded. Agencies are to ensure that they meet the requirements of the Privacy Act regarding collection of individually identifiable information. Such information is to be maintained and protected so as to preclude intrusion into the privacy of individuals. Individuals must be accorded access and amendment rights to records, as provided in the Privacy Act. Appendix I prescribes procedures for the maintenance of records about individuals in accordance with the Privacy Act.

In addition to Privacy Act considerations, statements (3) and (4) include provisions concerning proprietary information. Agencies are to minimize their collection of proprietary information, consistent with legal requirements and operational necessity and, when such information must be collected, agencies must provide for its protection.

(7). Training. Agency personnel must receive proper training to safeguard information resources. Training is particularly important in view of the changing nature of information resources management. The development of end user computing and office automation, for example, place the

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

management of information and information technology in the hands of nearly all agency personnel rather than in the hands of a few employees at centralized facilities such as large computer centers. Policies and procedures for computer security, records management, protection of privacy, and other safeguards need to be incorporated into information resources management training programs.

(8) through (12). Information Dissemination.

(8) and (9). General Policy. How does the public know what information is available from Federal agencies? That is, given the distinction the Circular makes between access and dissemination, what is the the relationship between the two? How does the public know what government information is accessible? The answer is: through the government's dissemination of information on what is available and how to gain to access it.

The Freedom of Information Act requires each agency to publish currently in the Federal Register, for the guidance of the public, descriptions of agency organization; where and how the public may obtain information; the general course and methods by which agency functions are determined, including all procedural requirements; rules of procedure; descriptions of forms and how to obtain them; substantive regulations; statements of general policy; and revisions to all the foregoing (5 U.S.C. 552 (a)(1)). The Privacy Act also requires publication of information concerning systems of records (see Appendix I); the Government in the Sunshine Act requires agencies to make public announcement of meetings (5 U.S.C. 552b (e)(1)). The Paperwork Reduction Act (44 U.S.C. 3507 (a)(2)) and Controlling Paperwork Burdens on the Public (5 CFR 1320) require agencies to publish notices when they submit information collection requests for OMB approval.

In sum, every Federal agency has obligations to disseminate basic information to the public concerning what the agency does, how its programs operate, what the public must do to comply with laws or regulations, how to receive benefits, and how the public can use agency services. These obligations are the basic linkage between access to, and dissemination of, government information.

Beyond generic requirements, specific laws affect agency dissemination of information in two ways. First, for some agencies their basic enabling legislation stipulates that information dissemination is part of their statutory mission. General purpose statistical agencies, for example, have information dissemination as part of their very reason for existence. These agencies conduct substantial information dissemination programs in order to carry out their necessary functions. In contrast, other agencies such as some regulatory agencies have basic information access, but minimal information dissemination, responsibilities; the existence of substantial information dissemination programs in such agencies would be

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

unusual. Second, statutes may sometimes require that agencies produce and disseminate specific information products or services. For example, the law may state that the President or head of an agency shall make reports to the Congress on given subjects; these would be legally required disseminations of information.

Beyond generic and specific statutory requirements, agencies have positive obligations to disseminate information as a necessary part of performing their functions. Each agency head must clarify the nature of these obligations for the agency's particular mission and set appropriate boundaries for dissemination functions. Before deciding to disseminate an information product or service, and periodically thereafter, an agency must be able to demonstrate that the dissemination of the product or service passes the test of either being required by law or being necessary for the proper performance of agency functions.

In conformity with the purposes of the Paperwork Reduction Act, the agency's positive obligations to disseminate information must be discharged within a responsible management framework of vinimizing costs to the Federal Government while maximizing the usefulness of the information. Efficient, effective, and economical dissemination does not translate into diminishing or limiting the flow of information from the agency to the public. To the contrary, good management of information resources should result in more useful information flowing with greater facility to the public, at less cost to the taxpayer.

Given an adequate basis for dissemination, agencies must also ask themselves whether a proposed or existing information product or service substantially duplicates similar products or services that would otherwise be available, either from another agency or from the private sector. This requirement of non-duplication, originating in the Paperwork Reduction Act, husbands scarce resources and leads to more efficient, effective, and economical information dissemination by the government.

Similarly, the fact that an agency has created or collected information is not itself a valid reason for creating a program, product, or service to disseminate the information to the public. Agencies create and collect much information, often for purely internal governmental purposes, that is not intended for dissemination, for which there is no public demand, and the dissemination of which would serve no public purpose and would not be cost-justified; e.g., compilations of routine time and attendance records for Federal employees, or publication of the thousands of pages of common carrier tariff filings by regulatory agencies. While such information may be subject to access upon request under provisions of agency statutes, the Freedom of Information Act, or the Privacy Act, the agency must demonstrate in each case the need actively to disseminate such information. Over time, changes in laws, economic conditions, or information

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

technology can result in changes in public demand, public purpose, or dissemination costs; for example, an agency's shift to electronic filing of reports, perhaps carried out primarily in order to improve internal information management, might generate a public demand for electronic dissemination that could be satisfied at minimal cost to the government and also improve the performance of the agency's information access function. The decision to disseminate information, however, entails potentially significant costs, must be addressed separately from the decision to create or collect information, and must hinge upon a determination that dissemination is necessary for proper performance of agency functions.

If agencies do contemplate disseminating particular information, they should plan for its dissemination when creating or collecting the information (see 8a(1)). Planning for dissemination should proceed from the Paperwork Reduction Act premises of minimizing the cost to the government while maximizing the usefulness of information. The focus of information dissemination plans should be on elevating to a policy level decisions regarding the agency's positive obligations to disseminate information and ensuring that the agency discharges the obligations in the most efficient, effective, and economical manner.

(10) Adequate Notice. Because many government information activities are important to the government and to the public, agencies must exercise care not to act capriciously with respect to information products and services. When agencies intend to commence offering new products or services, they should provide adequate advance notice so that the public may comment as to the need for the product or service. For example, if private sector interests believe they are already offering or are about to offer the same or a similar product or service--in which event the government may potentially be entering into unfair competition--such notice will allow these interests to present their case before the product or service is launched. By the same token, if many members of the public greatly depend on a particular product or service, they should be permitted to voice their views to an agency that is contemplating termination of the product or service.

The Circular refers to "significant" information products and services. It is not the Circular's intent that agencies should follow notice and comment procedures when terminating relatively inconsequential information products and services; examples might be minor brochures or flyers, products and services that were never intended to be continuing, or for which there is now little or no public audience. Agencies should determine for themselves whether information products and services are "significant," and in some cases may wish to establish procedures and threshold criteria for making such determinations. If a product or service

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

is considered significant, as determined ultimately by the agency head, the agency may be well advised to follow notice and comment procedures prior to initiation or termination.

(11)(a). Reaching the Public; Avoiding Information Monopolies. When agencies have justified and made the basic decision to disseminate information, they must also satisfy conditions regarding the manner of dissemination. First, agencies must take steps to ensure that members of the public whom the agency has an obligation to reach have a reasonable ability to acquire the information. The audiences for information products and services will vary, and agencies should tailor the dissemination methods so as to place the information into the hands of those whom the agency intends to receive it.

Federal agencies are often the sole holders of certain information; hence, when they disseminate, they are sole suppliers and in a position of natural monopoly. When agencies use private sector contractors to accomplish dissemination, they must take care that they do not permit contractors to exercise monopolistic controls in ways that defeat the agencies' information dissemination obligations, for example, by setting unreasonably high prices. In some cases agencies may need to formulate contractual terms with a sole supplier contractor so that the contractor functions as a mere intermediary for the agency in dealing with end users in the public.

(11)(b). Reliance on the Private Sector. In disseminating information--as with other activities--agencies must act in the most cost effective manner, which includes maximum feasible reliance on the private sector. This is merely an application to agency information dissemination programs of the policy stated in OMB Circular No. A-76, Performance of Commercial Activities, and summarized in Section 7f of this Circular. It is "the general policy of the government to rely on commercial sources to supply the products and services the government needs," including products and services the government needs in order to disseminate information to the public. For example, before an agency establishes a service for electronic dissemination of government information via an online computer system, the agency should compare the cost of contracting for operation of the service versus in-house performance and determine whether in-house performance is less costly both for the government and for the public who will receive the service.

Policies contained in OMB Circular No. A-76 are applicable to information dissemination, including the policy that inherently governmental functions should be performed by government employees. The general policy of reliance on the private sector is balanced by the "inherent governmental function" policy, and the Circular in no way intends to abrogate the latter. Where agencies determine that information dissemination activities are inherently governmental, the agencies themselves should carry out the activities.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(11)(c). User Charges.. The Federal Government is the sole possessor and supplier of certain types of information, which is frequently of substantial commercial value. Dissemination of such information, or its dissemination in a specific form or medium, may represent a government service from which identifiable recipients derive special benefits, in which case they may be subject to OMB Circular No. A-25, User Charges. For example, where the information is already substantially available in printed form, agencies may consider dissemination in electronic form to be a service of special benefit, the costs of which should be recovered through user charges. Many agencies do not have consistent, agency-wide policies and procedures for setting user charges for information products and services with a view to cost recovery. Agencies must establish user charges for the costs of information dissemination, and recover such costs, where appropriate. Whether user charges are appropriate depends, in principle, on whether identifiable recipients will receive special benefits from information products and services.

The requirement to establish user charges is not, however, intended to make the ability to pay the sole criterion for determining whether the public receives government information. Agencies must balance the requirement to establish user charges and the level of fees charged against other policies, specifically, the proper performance of agency functions and the need to ensure that information products and services reach the public for whom they are intended (see Section 8a (11)(a)). If an agency has a positive obligation to place a given product or service in the hands of certain specific groups or members of the public and also determines that user charges will constitute a significant barrier to discharging this obligation, the agency may have grounds for reducing or eliminating its user charges for the product or service, or for exempting some recipients from the charge.

(12). Periodic Review and Depository Libraries. Agencies must also establish procedures for periodically reviewing their information dissemination programs. Agency information dissemination plans must ask whether the agency should disseminate a given information product or service at all; if the agency is already disseminating the product or service, reviews should ask whether the agency should continue to do so; or whether the manner or medium of dissemination is the most efficient, effective, and economical.

In addition, agencies must establish procedures to ensure compliance with 44 U.S.C. 1902, which requires that government publications (defined in 44 U.S.C. 1901 and repeated in Section 6k of the Circular) be made available to the Federal depository libraries through the Government Printing Office. The depository libraries provide a kind of information "safety net" to the public, an existing institutional mechanism that guarantees a minimum level of availability of government information to all

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

members of the public. Providing publications to the depository library program complies with the law and costs executive agencies virtually nothing.

b. Information Systems and Information Technology Management. This subsection states policies concerning the planning, acquisition, operation, and management of Federal information systems and technology. The Federal information systems and technology budget, which was $14 billion in FY 1985, is projected to increase at a rate faster than that of the overall Federal budget. With outlays at these levels and agencies becoming increasingly dependent upon information technology to accomplish their missions, it is essential that planning processes be applied to the acquisition and application of information technology.

(1). Planning. The Paperwork Reduction Act mandates a stronger central role in information resources planning. Specifically, the Act requires that OMB: (1) publish a five-year government-wide automatic data processing and telecommunications plan; (2) review and coordinate agency proposals for the acquisition and use of information technology; and (3) promote the use of the technology to improve governmental efficiency and effectiveness. In order to meet these objectives, it is necessary to initiate a government-wide process for developing and institutionalizing information technology planning that is based in agency programs and missions. The planning must also be tied to the budget so that budgetary decisions derive from plans, and conversely, so that budgetary constraints are reflected in the plans. The process must further ensure that sufficient information is available to the central agencies to enable them to monitor compliance with Federal policies and identify major issues, including cross-cutting issues where more active centralized planning and management may be appropriate. Hence, agencies must institute information planning processes tied to both the conduct of programs and the preparation of the agency's budget.

(2) and (3). Management Controls and Accountability. Basic management controls for agency information systems are fundamental to sound information resources management. These controls should ensure the documentation and periodic review of major information systems, as well as periodic cost-benefit evaluation of overall information resources management in light of agency missions. In order to provide greater incentive for management efficiencies, accountability for information systems should be vested in the officials responsible for operating the programs that the systems support.

Program managers depend upon information systems to carry out their programs, and yet frequently they do not have direct control over the technical and operational support for those systems. Program managers often depend upon agency computer centers or contracted service organizations, the heads of which

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

may not be directly accountable to the program managers in a formal organizational sense. Program managers are nonetheless responsible for conducting their programs and, to the extent successful conduct of the programs entails support from information systems, program managers must be held accountable for acquiring that support. The responsibilities of program managers are therefore presumed to include securing information systems support as needed, and planning for contingencies. Technical support organizations have a concomitant responsibility to meet their commitments, contractual or otherwise, to their program clients, but the program official has the ultimate responsibility for delivering a program's product or service.

(4) and (5). Sharing Information Processing Capacity. OMB Circular No. A-121, which is rescinded and superseded, required only that the holder of excess automatic data processing capacity share such capacity. Because the holder of excess capacity has little incentive to seek opportunities for sharing, however, the new policy requires both that the holder share capacity and that the agency seeking information processing capacity fulfill its needs from other agencies or the private sector, whenever possible, before acquiring the new capacity itself. The policy establishes an order of preference in meeting needs--look first to existing sources before acquiring new capacity--but is not intended to assert blindly that sharing or commercial sources are the sole considerations. Agencies must also consider whether existing sources are more cost effective and whether they in fact will meet agency specific needs. Procedural aspects of these policy statements are found in Appendix II.

(6) and (7). Life Cycle Costing; and Avoiding Duplication. Agencies frequently develop information technology incrementally, through a series of interim upgrades, without regard for longer term considerations such as the information systems' life cycle. As part of their planning, agencies need to consider the full information system life cycle when determining the cost of information technology. While competitive procurement is generally to be valued, its costs should be taken into account, including the cost to program effectiveness of unnecessarily lengthy procurement processes. Other conditions, such as the need for compatibility, may also be legitimate limitations on the competitive process. Similarly, agency planning should ensure that information systems are not unnecessarily duplicative of systems available elsewhere in government or from the private sector.

(8). Software Management. The prevailing agency practice of developing customized computer software is a source of inefficiency, as the General Accounting Office and others have noted. While some agency applications can only be satisfied with customized software, the tendency to prefer custom development is excessively costly in terms of initial development, continued maintenance, and eventual conversion to new technology, because

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

it requires the agency to bear the full cost of developing and maintaining the software it uses. While recognizing that off-the-shelf software has pitfalls, such as uncertainty of continued maintenance, managers are generally to prefer acquiring generic, off-the-shelf software available from the private sector instead of developing their own.

(9). Necessary Compatibility. Agencies often acquire technology that is incapable of communicating with other systems with which the agencies need to communicate. Compatibility among information systems has consequently emerged as a significant information resources management problem. Agencies must acquire or develop information systems in a manner that enhances necessary compatibility. The qualifier "necessary" is used because compatibility is not an unrestricted goal; information systems need to be compatible with other systems only to the extent that they must communicate with those systems.

(10) through (13). Security. Security of information systems means both the protection of information while it is within the systems and also the assurance that the systems do exactly what they are supposed to do and nothing more. Information system security entails management controls to ensure the integrity of operations including such matters as proper access to the information in the systems and proper handling of input and output. In this sense, security of information systems is first and foremost a management issue and only secondly a technical problem of computer security.

The recent introduction of smaller and more powerful computer systems and new communications technology and transmission media, together with the greater involvement of end users in managing information resources, have increased the potential vulnerability of Federal information systems and hence the level of management concern. Protecting personal, proprietary, and other sensitive data from unauthorized access or misuse; detecting and preventing computer related fraud and abuse; and assuring continuity of operations of major information systems in the event of emergency related disruptions are increasingly serious policy issues. Policy previously found in Transmittal Memorandum No. 1 to OMB Circular No. A-71 is here revised; procedural aspects of the policy are in Appendix III to the Circular.

The General Accounting Office reported in its review of the first-year implementation of the Federal Managers Financial Integrity Act (FIA) that internal controls in automatic data processing systems received inadequate coverage in FIA evaluations. GAO noted that some agencies were uncertain of the relationship between (a) OMB Circular No. A-71, Transmittal Memorandum No. 1, Security of Federal Automated Information Systems, and (b) OMB Circular No. A-123, Internal Control Systems. The relationship between security of automated information systems and agency internal control reports is now stated clearly in Appendix III.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Appendix III provides a minimal set of requirements for the security of all Federal automated information systems. The Appendix also requires agencies to incorporate additional requirements for the security of information classified for national security purposes, in accordance with appropriate national security directives.

(14). Standards. The National Bureau of Standards, Department of Commerce, develops and issues Federal Information Processing Standards. The National Communications System develops and the General Services Administration issues Federal Telecommunications Standards. Some standards are mandatory for Federal agencies, while others are voluntary. Agencies may waive the use of Federal standards under certain conditions and pursuant to certain procedures, which vary depending upon the individual standard. In general, OMB strongly recommends use of these standards government-wide. Such standards can contribute to overall government economy and efficiency by increasing compatibility in computer and telecommunications networks, improving the transportability of software, and enabling computer systems to be developed using components of different manufacturers. These advantages can result in reduced procurement costs for equipment and services, improved competition, and better utilization of staff training and skills. While government-wide standards can result in management efficiencies, agencies should be mindful that standards can also have the untoward effects of regulations, as noted in OMB Circular No. A-119. Agencies should continuously assess relative costs and benefits of standards and their effects upon the agency's accomplishment of its mission. Note also that national security directives prescribe standards for computer security.

(15) Avoiding Information Technology Monopolies. Many agencies operate one or more central information technology facilities to support agency programs. In these agencies, program managers are often required to use the central facilities. The manager of such a monopoly facility has a lesser incentive to control costs, since he or she has a captive clientele. The program manager has little leverage to ensure that information processing resources are efficiently allocated since he or she cannot seek, or can seek only with great difficulty, alternative sources of supply. When users are dependent on effective technology support to perform their functions, control over selection of facility is essential and consistent with holding users responsible for producing their government information products. To provide incentives conducive to more businesslike procedures in information technology facilities, agencies should avoid monopolistic information processing arrangements and should enter into them only if their cost effectiveness is clear and they are subject to periodic review. Appendix II specifies certain procedures with respect to this policy.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

(16) Cost Recovery. This policy constitutes a revision to policy stated in OMB Circular No. A-121. Whereas Circular No. A-121 required only that costs for automatic data processing facilities be allocated to users, agencies must now recover the costs of information technology facilities from government users. Viable management of a large information technology facility requires that managers know the amount of resources devoted to each user when providing services. Furthermore, effective management of the use of information technology requires that the user have responsibility for and control over the resources consumed by use of the facility. Experience with Circular No. A-121 showed OMB that allocating costs had little effect on agencies' behavior; recovering costs means that actual transfers of funds will take place between suppliers and users of information technology facilities. Procedural aspects of the policy appear in Appendix II.

(17) Coordination with State and Local Governments. This policy reaffirms policy previously found in OMB Circular No. A-90, Transmittal Memorandum No. 1. The interagency group that worked on the revision of Circular No. A-90 recommended, and OMB agreed, that the Circular should be rescinded except for a single policy statement prohibiting Federal agencies from placing unnecessary restrictions on the information systems that State and local governments use to carry out federally financed program activities.

(18) Application of Up-to-date Information Technology. Recent availability of low cost, highly efficient and effective electronic information technology can greatly increase worker productivity and facilitate operation of Federal agency programs. The Circular states a predisposition, based in the Paperwork Reduction Act, in favor of applying such technology to the information life cycle within a responsible management context. Two broad areas of information technology merit further discussion: (1) electronic information collection and dissemination, and (2) end user computing.

- Electronic Collection and Dissemination of Information. Federal agencies are moving rapidly to provide for collection and dissemination of information through electronic media. In developing this Circular, OMB considered whether it was necessary to provide specific policies concerning electronic collection and dissemination of governmental information. OMB concluded that, except for the general predisposition in favor of applying new technological developments to information resources management, the policies that apply to information collection and dissemination in other media also apply to electronic collection and dissemination. It is important, however, that agencies recognize the necessity of systematically thinking through the application of policies stated elsewhere in this Circular to electronic collection and dissemination of information. For example, when developing electronic collection programs, agencies

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

should give particular attention to issues such as privacy, public access, and records management.. When developing electronic dissemination programs, agencies should ensure that access is provided to each class of users upon reasonable terms, avoid problems arising from monopolistic control, ensure maximum reliance upon the private sector, and take necessary steps for cost accounting and cost recovery.

- End User Computing. Federal agencies are also moving rapidly to acquire end user computing capabilities. OMB endorses the managed innovation approach to end user computing presented in GSA's publication Managing End User Computing in the Federal Government (June 1983). Because end user computing places management of information in the hands of individual agency personnel rather than in a central automatic data processing organization, the Circular requires that agencies train end users in their responsibilities for safeguarding information; Appendix III deals in part with the security of end user computing.

Section 9. Assignment of Responsibilities.

This section assigns responsibilities for the management of Federal information resources addressed in this Circular. OMB Circular No. A-71 is rescinded and its contents are revised and incorporated into this section along with responsibilities assigned under the Paperwork Reduction Act; Section 111 of the Federal Property and Administrative Services Act, as amended; and Executive Order No. 12046. Certain assignments of responsibility from OMB to other agencies, as noted below, are also included. Following are principal noteworthy aspects of this section.

Responsibility for Managing Information Resources. Statement 9a(1) is a key element in the Circular because it establishes that the locus of responsibility for actual management of Federal information resources is the head of each agency. This means, for example, that the determination of what is "necessary for the proper performance of agency functions" with respect to information creation or collection (8a(1)) and information dissemination (8a(9)) lies with the head of the agency. In the Circular OMB sets the policy framework within which such determinations are to be made and the standards and provisions for reviewing the determinations, but the management decisions and their implementation belong properly with the agency holding the information resources.

Triennial Reviews. The Paperwork Reduction Act provides that the Director of OMB ". . . shall, with the advice and assistance of the Administrator of General Services, selectively review, at least once every three years, the information management activities of each agency to ascertain their adequacy and efficiency." (44 U.S.C. 3513) The Administrator of Information and Regulatory Affairs, OMB, and the Deputy Administrator of the General Services Administration, in an

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

exchange of correspondence dated June 13 and July 22, 1983, concurred that GSA has the necessary statutory authority to conduct reviews of Federal agency information resources management activities. Separate triennial reviews of agency activities by OMB and GSA would be unnecessarily duplicative, which would not be consistent with the Act. Accordingly, the triennial reviews conducted by GSA will be designed to meet OMB's requirements under the Paperwork Reduction Act as well as GSA's own needs.

Senior Officials for Information Resources Management. In accordance with 44 U.S.C. 3506(b) and 5 CFR 1320.8, agencies are required to designate a senior official to carry out responsibilities under the Paperwork Reduction Act. The designation of the official is intended to assure clear accountability for setting policy for agency information resources management activities, provide for greater coordination among the agency's information activities, and ensure greater visibility of such activities within the agency. The responsibilities of the senior official for information resources management were identified in OMB Bulletin No. 81-21, which has expired. Those responsibilities are now established in this Circular.

International Information Policy. The Circular deals with the management of information resources held by the Federal government. While the creation, collection, processing, transmission, dissemination, use, storage, and disposition of information by the Federal government has international ramifications, Federal government information resources management policy is not the same as "U.S. information policy," which refers to U.S. national interests in the information field vis-a-vis the policies and interests of other nations. The Circular formally acknowledges this distinction and assigns responsibilities for international information policy only insofar as it relates to Federal government information resources management policy.

Timely Technology Procurement. Inherent in effective management of information technology is the ability of program managers to acquire technology in a timely manner. GSA is assigned the responsibility in Section 9 to develop criteria that will streamline procurement procedures and delegate procurement authority to agencies that comply with those procedures. All Federal agencies are directed in Section 9 to develop internal policies and procedures that further provide for timely acquisition of information technology.

Records Management. The Paperwork Reduction Act makes the management of Federal records an integral part of information resources management. While no new policies are embodied in this Circular, responsibilities have been assigned in order to ensure that agency records management programs are considered within the context of Federal information resources management.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1

Section 10. Oversight.

The broad scope of the Circular dictates a strategy of focusing oversight on a series of aspects of information resources management rather than on a single comprehensive reporting scheme. OMB intends to use existing mechanisms, such as the fiscal budget, information collection budget, and management reviews, to examine agency compliance with the Circular. For example, during 1984 the management reviews for the FY 1986 budget year concentrated on five cross-cutting information issues: overall information resources management strategy, telecommunications, software management, "electronic filing," and end user computing. OMB issued data call bulletins requesting information specific to these issues, targeted the issues for special attention during the management reviews, and requested individual agencies to submit management improvement plans on specific aspects of the issues. Pursuit of this kind of selective oversight strategy permits OMB and the agencies the flexibility to shift the focus of oversight as information issues and the technological environment change.

Sanitized Copy Approved for Release 2010/04/23 : CIA-RDP87M01152R000300360004-1